

Application of cloud computing in banking and e-commerce and related security threats

Ranjan Kumar Mondal

Swami Vivekananda University

ranjankm@svu.ac.in

Abstract

One of the most potent innovations that has piqued the interest of technologists worldwide is cloud computing. Although cloud computing offers several benefits, there are numerous security threats that no company can afford to overlook. Effective planning and knowledge of new risks, threats, vulnerabilities, and potential solutions are essential for a company to implement cloud computing successfully. Determining the best solution guidelines to boost cloud security has, therefore, become crucial for all cloud operations. Based on a survey of the literature, we are examining and evaluating the most significant network security and data security threats to cloud systems in this study. A closer analysis reveals that virtualization introduces more software to the network system, which might have a detrimental impact on security if poorly designed and implemented. This is because many firms have advertised and pushed virtual environments as the answer to today's security issues. Additionally, data center hubs connect their servers via software, which might have a negative impact on security if something goes wrong. Because they have no control over the cloud's resources, consumers must rely on trust mechanisms.

Introduction

E-learning, healthcare, and e-commerce are just a few fields impacted by cloud computing. It provides cost-effective, high-quality internet services that hold

significant economic value. Without a doubt, this is the next big trend in business and the internet. To maximize practical value, more e-commerce companies are shifting to cloud computing. Any analysis of a public scheme begins with the classification of concepts and attitudes. Numerous approaches to cloud computing exist, according to a review of recent and innovative literature, which offers the following operational descriptions: According to NIST, (National Institute of Standards and Technology), “cloud computing” (or simply “cloud”) is a new term that encompasses how multiple contemporary computing techniques and technologies have evolved into something new [7,8]. The cloud separates application and information resources from the underlying infrastructure and delivery methods. According to Barkley RAD, “Cloud computing refers to both the applications provided as services over the Internet and the hardware and systems software in the data centers that enable those services.” For many years, Software as a Service (SaaS) has been a prevalent model. The data center’s hardware and software constitute the cloud. When a cloud is made available to the general public for a fee, it is termed a public cloud. Utility computing offers such services. The term “private cloud” describes the internal data centers of a company or organization that are inaccessible to the public. Hence, private clouds are not part of the overall SaaS and Utility Computing Cloud Computing system. Individuals can be producers, consumers, or users of SaaS [1].

One of the most significant innovations that has garnered the interest of technologists worldwide is cloud computing. While cloud computing provides numerous benefits, including scalability, rapid flexibility, measurable services, and – most notably – the potential for cost reductions for businesses, it also introduces various security risks that no company can afford to ignore. The wide array of vulnerabilities inherent in every cloud computing system raises security concerns. In the absence of robust security

policies, businesses seem hesitant to leverage the otherwise robust environment of cloud computing [2]. Figure 1 illustrates the benefits of cloud computing. By separating information and application resources from the fundamental infrastructure and mechanisms used to deliver them, “cloud computing” fundamentally describes the evolution of many current technologies and methods in computing, incorporating resource allocation into utility models and elasticity. Cloud computing helps businesses and consumers save money while enhancing collaboration, scalability, availability, and agility. In summary, cloud computing involves the utilization of various applications, data and infrastructure, networks, storage resources, and, ultimately, distributed services [3].

Utilizing a utility model for allocation, relocation, and consumption, these components can be easily arranged, provided, implemented, and dismantled. Although cloud computing has significantly benefited individuals and businesses with features like scalability, rapid elasticity, measurable services, and multi-tenancy through automation, virtual presence, and service availability, serious security threats have emerged in recent years, such as network security and data privacy issues [4].

Larger businesses still don’t fully trust that their online bulk data will remain confidential. For a corporation to successfully implement cloud computing, careful planning and awareness of new risks, threats, vulnerabilities, and viable solutions are essential. A key aspect of secure cloud computing will involve creating reliable programs from unreliable components. While businesses may be able to save money by leveraging cloud computing, significant security risks remain that require careful attention [5].

Due to the sensitive nature of cloud computing architecture, specific security concerns have arisen. Therefore, assessing cloud networks to identify security threats and vulnerabilities is crucial. The large-

scale deployment of cloud computing necessitates evaluating vulnerabilities and attacks and designing appropriate solutions to enhance security and privacy in the cloud environment [6].

Characteristics of Cloud Computing Technology

On-demand self-service: Customers can request computing capabilities or resources, such as server time and network storage, as needed without requiring human intervention or interaction between the user and each cloud service provider. In other words, a company will acquire cloud-hosting services from a cloud-host provider, which may be a usual software vendor. Customers have access to these services, and

The ability to modify cloud services, such as computing and storage, as needed through an online control panel or directly with the provider, as well as to manage and deploy these services [7].

Ubiquitous network access: Cloud Computing / Broad Network Access: All features are accessible via the network and may be accessed using standard methods that facilitate use by a variety of thin and thick client platforms, including laptops, tablets, mobile phones, and workstations. To put it another way, the group may access company management systems via their tablets, smartphones, laptops, office PCs, and workstations. Anyone may use these gadgets from anywhere as long as they have an essential connection to an online access point. Because it enables workers to stay on top of contracts, projects, and clients whether they are in the office or not, this mobility appeals to enterprises.

Location-independent resource pooling: Through a multi-tenant approach, the provider's computer resources are combined to service a large number of customers, with different virtual and physical resources being dynamically assigned and reallocated in response to customer demand. Although the client can designate the location of the supplied resources at a higher level of abstraction, such as data center, region, or country,

which includes resources like processor, memory, storage, and network bandwidth, they have no control over or knowledge of the precise location of these resources.

Rapid elasticity: It describes the ability of the cloud to quickly and efficiently increase or decrease allocated resources to meet the needs of the self-service aspect of cloud computing. The user would see a vast pool of dynamic resources that could be paid for as required, and this allocation could be completed automatically. One element that enables quick elasticity is the development and implementation of loosely connected services that scale independently of other services and are not reliant on the elasticity of these other services.

Measured service: Cloud systems use metering capabilities at an abstraction level appropriate for the kind of service to control and optimize resource use automatically. Both the provider and the customer may benefit from transparency by being able to track, control, and report on cloud resource usage. You pay for what you use, thanks to the cloud's low cost. You and your cloud provider can appropriately assess and bill for storage, processing, bandwidth, and user accounts. The amount of resources you can use can be monitored and controlled by your cloud provider as well as by you, ensuring transparency [8]. Features of cloud computing technology are depicted in Fig. 2.

Applications of Cloud Computing in Banking and E-Commerce

Key applications [6–8] of cloud computing in banking and e-commerce include:

Open-Access Commercial Online Banking Portals : This technology represents the evolution of commercial online banking, enabling users to access a comprehensive suite of services, products, and information, some provided by the bank and others by third parties.

Widget-Based Internet Banking Applications :

These innovative solutions for retail banking allow users to personalize their online banking interface and interact with products and information using widget-based technology.

Mobile Retail Stock Trading : This approach allows retail investors to perform stock transactions via mobile devices, such as smartphones or PDAs, excluding laptops or tablets.

Self-Service Applications for Commercial Customers : This technology focuses on creating commercial self-service portals and tools, empowering banks to deliver quick, detailed information to business clients and assisting them in making informed management decisions.

Advantages of Using Cloud Computing in Banks

The following are the advantages of utilizing cloud computing [9,10] in banking:

- **Cost savings and usage-based billing :** Financial institutions can use cloud computing to convert a hefty upfront capital expense into an economical, ongoing operational cost. They can avoid substantial investments in new hardware or software while selecting services on a pay-as-you-go model.
- **Business Continuity :** With cloud computing, providers manage the technology, enhancing data protection, fault tolerance, and disaster recovery. This offers superior redundancy and backup capabilities at a lower cost compared to traditional systems.
- **Business Agility and Focus :** Cloud-based operational models allow financial institutions to accelerate product development cycles, enabling quicker and more effective responses to client needs. As cloud services are available on-demand, less infrastructure investment is required, facilitating

faster deployment. Moreover, companies can shift non-essential tasks like software maintenance to the cloud, allowing them to concentrate on core financial services. Additionally, transitioning services to a virtual environment helps reduce energy consumption and minimize the carbon footprint linked to physical infrastructure.

Threats to E-Commerce

E-commerce encompasses the buying and selling of goods online, pertaining to commercial transactions conducted over the Internet. E-commerce technologies include:

- Mobile commerce.
- Internet marketing.
- Online transaction processing.
- Electronic funds transfer.
- Inventory management systems.
- Automated data collection systems.

E-commerce threats involve the misuse of the Internet for unethical purposes like theft, fraud, and security breaches. These threats vary in nature, including unintentional risks, deliberate attacks, and human errors. Common electronic payment threats are e-cash fraud, data abuse, credit and debit card fraud, and various security vulnerabilities [11–14].

Security Challenges & Issues in Cloud Computing for Banking and E-Commerce

Several security concerns related to cloud computing technology [15–19] include:

i. Multi-tenancy refers to shared access to physical resources or devices and virtualized software resources among multiple independent clients and organizations.

ii. Analyzing sensitive information is risky, as security breaches can occur in cloud environments while monitoring significant activities like new execution processes or file creations.

iii. Semantic Gap: Extracting meaningful information from low-level data is crucial.

iv. Loss of Control: Clients relinquish physical ownership of their data stored in the cloud. Cloud providers may possess sensitive information and could potentially mine customer data, which could lead to breaches. Clients who delete data from a cloud provider that backs up at several centers cannot be assured of complete deletion. This creates a perception of cloud services as “black boxes” where clients cannot freely monitor their data.

v. Trust is essential, as it determines user willingness to embrace cloud services despite the loss of physical control over their data. Consequently, companies are working to build confidence through certified compliance with security standards.

vi. Attacks on virtual architecture pose significant concerns, and there is an increased risk of information-driven buffer assaults on untrusted cloud systems.

vii. In real-life digital applications, performance quality is always a critical factor. Therefore, adequate security is favorable when performance metrics align with customer and administrator expectations.

Conclusion

Successful cloud computing adoption in organizations requires careful planning and a thorough understanding of emerging risks, threats, vulnerabilities, and workable solutions. In our research, we analyze and assess the most significant network and data security threats to cloud systems, which are based on a review of the literature. Since many firms use virtual environments to explore and publish their answers to modern security issues, a

closer look reveals that virtualization adds additional software to the network system, which might negatively impact safety if it is poorly designed and implemented. Furthermore, data center hubs use software to connect their servers, which might compromise security if something goes wrong. Customers must have faith in the service provider because they have no control over cloud resources. This article discusses several cloud applications and associated security concerns in e-commerce and banking.

References

A. Fernandez, E. Insfran, S. Abrahão, Usability evaluation methods for the web: A systematic mapping study, *Inf. Softw. Technol.* 53 (2011) 789–817, ISSN 0950-5849.

M. Scalera, A. Serra, Customer-centric strategies for value creation: Academic experimentation, *J. E-Learn. Knowl. Soc.* (2014) 10.

P. Mell, T. Grance. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology; National Institute of Standards and Technology Laboratory: Gaithersburg, MD, USA, 2011; Volume 145, p. 7.

D. Folinas, I. Manijas, D. Graham. E-Logistics and E-Supply Chain Management: Applications for Evolving Business, 1st ed.; IGI Global: Hershey, PA, USA, 2013; ISBN 9781466639140. M.R.C. Dr. Sheel Ghule, Mr. Kalpesh Parmar, “Cloud Computing In Banking Services,” *International Journal Of Scientific And Research Publications*, Wwww. Ijsrp.Org, Vol. Volume 4, June 2014.

N.M. Abdelrafe Elzamly, Mohamed Doheir, Ahmed Mahmoud, N. A. S. Abd Samad Bin Hasan Basari, Sayed Samer Ali Al-Shami, “Adoption Of Cloud Computing Model For Managing EBanking System In Banking Organizations,” *International Journal Of Advanced Science And Technology*, Vol. Vol. 28, No. 1, Pp. Pp. 318-326, (2019),.

Ulrich Lampe, Olga Wenge, Alexander Müller, And Ralf Schaarschmidt, "Cloud Computing In The Financial Industry – A Road Paved With Security Pitfalls," Proceedings Of The Eighteenth Americas Conference On Information Systems, Seattle, Washington, August 9-12, 2012, 2012.

L.M.S. Gayatri Sattiraju, Shakti Mishra, "Idrbt Community Cloud For Indian Banks," 2013 international conference on advances in computing, Communications and Informatics (Icacci), 978-1-4673-6217-7/13/\$31.00 C 2013 IEEE.

J.Y. Abhishek Mahalle Xiaohui Tao, Jun Shen, "Privacy And System Security For Banking And Financial Data Privacy And System Security For Banking And Financial Services Industry Based On Cloud Computing Infrastructure Services Industry Based On Cloud Computing Infrastructure," Putting Infrastructure" Faculty Of Engineering And Information Sciences - Papers: Part B. 1357, (2018).

K.S.T. Mayank Singh¹, Viranjay M. Srivastava³, "Cloud Computing Adoption Challenges In The Banking Industry," 978-1-5386-3060-0/18/\$31.00 ©Ieee, 2018

D.H. Tesema, "Cloud Computing Adoption Challenge In Case Of Commercial Bank Of Ethiopia" International Journal Of Development Research, January 2020, Vol. Vol. 10, Pp. Pp. 33562- 33565, January, 2020.

X.R.L. Ranjit Bose, Yuan Liu, " The Roles Of Security And Trust: Comparing Cloud Computing And Banking," The 2nd International Conference On Integrated Information 2013

C.M. Thakar, S.S. Parkhe, A. Jain et al., 3d Printing: Basic principles and applications, Materials Today: Proceedings, <https://doi.org/10.1016/j.matpr.2021.06.272>

V. Panwar, D. Kumar Sharma, K.V. Pradeep Kumar, et al., Experimental investigations and optimization of surface roughness in turning of en 36 alloy steel using response surface methodology and genetic algorithm,

Materials Today: Proceedings, <https://doi.org/10.1016/j.matpr.2021.03.642>

M. Kaosar Ahamed, A. Babu, S. Babu et al., Layout map in facility layout planning: A fuzzy methodology, Materials Today: Proceedings, <https://doi.org/10.1016/j.matpr.2021.06.091>

N.S.S.A. D.P. Sharma², “Cloud Computing Security Through Cryptography For Banking Sector,” Proceedings Of The 5th National Conference; Indiacom-2011 Computing For National Development, March 10-11, 2011 Bharati Vidyapeeth’s Institutes Of Computer Applications And Management, New Delhi, Copy Right © Indiacom-2011.

S.R.A.A. Gangal², “Security Issues Of Banking Adopting The Application Of Cloud Computing,” International Journal Of Information Technology And Knowledge Management, Vol. , Volume 5, No. 2, Pp. Pp. 243-246, July- December 2012.

G.O. Martin Shikuku Gwara¹, Michael Kimwele³ 1, “A Framework For Assessing Cloud Computing Security For Cloud Adoption In Microfinance Banks,” International Journal Of Advances In Computer Science And Technology, 3(1), January 2014, 34 - 38, Vol. Volume 5 No.11, , November 2016.

S.T. Jagtap, C.M. Thakar, O. El Irani, K. Phasinam, S. Garg, R.J.M. Ventayen, “A Framework for Secure Healthcare System Using Blockchain and Smart Contracts,” 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC), 2021, pp. 922-926, doi: 10.1109/ICESC51422.2021.9532644.